

Claims

- [c1] A method of backing up one or more files on a local device onto remote servers over a network comprising:
- deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
 - compressing one or more files and adding each of the files to a bundle;
 - generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and
 - encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server.
- [c2] The invention of claim 1 wherein the bundle is encrypted using a strong block cipher.
- [c3] The invention of claim 1 wherein the authentication code is an HMAC.
- [c4] The invention of claim 1 wherein the cryptographic keys contain at least 128 bits.
- [c5] A method of restoring one or more files on remote servers to a local device over a network comprising:
- deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
 - decrypting a bundle received from the remote server using the second cryptographic key;
 - checking an authentication code in the bundle using the first cryptographic key; and
 - decompressing one or more files from the bundle;
- [c6] The invention of claim 5 wherein the bundle was encrypted using a strong block cipher.
- [c7] The invention of claim 5 wherein the authentication code is an HMAC.
- [c8] The invention of claim 5 wherein the cryptographic keys contain at least 128 bits.

09632526.091401

- [c9] A device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network, the method comprising the steps of:
- deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
 - compressing one or more files and adding each of the files to a bundle;
 - generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and
 - encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server.
- [c10] The invention of claim 9 wherein the bundle is encrypted using a strong block cipher.
- [c11] The invention of claim 9 wherein the authentication code is an HMAC.
- [c12] The invention of claim 9 wherein the cryptographic keys contain at least 128 bits.
- [c13] A device-readable medium storing program instructions for performing a method of restoring one or more files on remote servers to a local device over a network, the method comprising the steps of:
- deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
 - decrypting a bundle received from the remote server using the second cryptographic key;
 - checking an authentication code in the bundle using the first cryptographic key; and
 - decompressing one or more files from the bundle;
- [c14] The invention of claim 13 wherein the bundle was encrypted using a strong block cipher.
- [c15] The invention of claim 13 wherein the authentication code is an HMAC.
- [c16] The invention of claim 13 wherein the cryptographic keys contain at least 128

bits.

09637526.094401